

Ken Delaney – **Technology and Management Directions for Smartphones and Tablets**

Attempts by businesses to ban, discourage and control the use of these devices have been unenforceable. Businesses do not need tablets and smartphones to function for increased productivity – a laptop and a phone are still good enough to use. This market is exploding because the end user is dictating what they want, and IT Departments are not. There is no documented business argument for integrating tablets into your environment – they are useful, but you can do all your work with current tools. **BUT** the more IT pushes the organization standards the more employees will go outside to find the tools they want which opens up security holes.

There is a war (ARM processors – that have OS that are different than Microsoft) and the products revolve around the browser and now companies like HP are moving their OS on PCs and there is now a battle in the PC market. The concerns with standardization and enterprise management we are having today will bleed into the Netbook and laptop market as vendors move to Browser Operating Systems.

Development -There isn't a lot of innovation in the ergonomics – form factors have stabilized (clamshell, convertible, open-face, hybrids [wearables]) so the efforts are being made in application development. This is different for the marketplace than previously seen.

For example – **applications** - In 2011 the technology is being used for business for mobile payments. This is just going to get bigger and our currency is changing. Mobile devices (with web services) have now been integrated into common electronic equipment (clock radio with iPad adaptor), car starters, etc. If you have a website today – you must be sure it is accessible from mobile devices as this is going to be one of the primary access tools.

The Measurement of Great Tablets (criteria) – Motorola Xoom – they have dual core processors, wifi versions less than \$500.00, instant on, self contained, 16 x 9 tablet screens with thinner bezel (7 inch is too small and not 16 X10- too big), intuitive user interface, video camera integrated, > 30,000 apps availability benchmark (there are claims that apps for android will work on any device – this is not true).

Is the iPhone beatable? If you look at what makes a great tablet they have these and they are rated A+ in all and they are great marketers. Google has very fragmented advertising because they are letting the device manufacturers do the work. Google is now trying to catch up.

Android is becoming the number one (Nokia's is now number 2 BUT- Symbian is being phased out for Windows Phone 7 – which will make a significant challenger), iPad is Number 3, RIM is 4 and losing share (but the Curve is very popular) because they do not have a good tablet but they have made some good purchases lately (will take them 9-12 months).

Linking to Web Services is the new Battleground – Issues:

- Security – where is our information?
- Single Point of Failure

Foundation of Context and Collaboration – Why these devices are so different and the use is changing how we work:

- The user says who they want to collaborate with and the system figures out the best way for the user to do that. The system also decides the context that you receive the information through. Rather than the user going to get them (Google search is no longer) – example as you enter a store, the coupons are sent to your device.
- Mobile collaboration client – multiple data sources in a single view with multiple layers (Apple is slow to this – but gearing up).

Cornerstones of Management – what can we do?

Standards were in place, but these devices are forcing changes -

- Security, patch management, governance, risk and compliance, inventory – cost has to be co-located not just the IT group because they will not have the authority of the device.
- Access and roaming control – as users get onto different networks the system has to ensure that they have to correct system – this is coming.
- A device has to be capable of being cleaned of all content "over the air" (OTA), should the device be reported as lost or stolen.
- Forces the user to employ a complex password consisting of a combination of uppercase and lowercase letters, numbers and special characters, with the ability for periodic changes.
- Encryption is now a suggested option for appliance-level devices. If a device meets the above baseline security requirements and has an encryption capability, it should be invoked as an extra measure of protection. This is suggested even when it causes some user inconvenience, slight performance degradation or has not been proven in all tested security scenarios. Encryption will remain a suggested option until YE11, at which time, Gartner believes, most mainstream endpoint operating systems with at least 10% share of their respective market will have robust solutions. At that time, we expect to make encryption mandatory.
- Organizations that permit individually liable devices to connect to enterprise e-mail systems under the appliance level must require the user to sign documents that enforce at least three policies:
 1. As a condition of employment, the end user must report any lost or stolen device to IT immediately upon detection.
 2. When reported lost or stolen, the user grants permission for the device to be wiped of its contents. This policy is necessary to ensure that an end user who has invested in personal music, but who hasn't backed it up, doesn't make a compensatory claim for reimbursement.
 3. And, lastly, to prevent misuse, users must be told that these devices are for their own convenience, but that all e-mail and attachments must be read on standard PCs and notebooks. This prevents the user from believing that a mobile or other non-PC endpoint device is a notebook substitute and blaming IT for any document conversion mistakes inherent in non-Windows platforms.

Managed Diversity Model – Why this model? – a homogeneous environment in which everyone has the same device is difficult if not impossible to achieve and maintain.

- IT controlled - Establish a platform support level that permits a narrow set or single choice of hardware when enhanced application support is required. If you want IT to be responsible for the device – then IT has to dictate what is purchased.
- Shared IT responsibility – Establish an appliance support level for a broader set of hardware choices when applications can be constrained to support solely voice, email, personal information management and selected applications that run consistently.
- Concierge – move to individual purchases (individual liable devices) or additional hands on custom support costs for a fee.
- Combine all three to form a managed diversity matrix for up to 7 groups. Break up the user community into groups with similar needs, and then provide each user in a given group with a portfolio of devices, applications, services and privileges identical to the group – this is not cost effective as user circumvents policies leaving IT department to support personally owned machines.

With these you have cost control and auditable security that have to be considered.

Enterprise Management of Devices – Windows Platforms as opposed to Android and IOS - What is the difference technically -

The tablet – the application can only see its BIOS section so it is impossible for a single application to monitor the entire environment. The user has to be involved.

Apple – IOS devices – Personal device – third party management server allows access – there is a certificate put in the device and then whenever there is an app downloaded the app is given a key on the device so there is no split. To remove device – then remove the certificate and all applications go away (this is new). This is “Over The Air” (OTA) cleaning of content in case a device is lost or stolen.

All updates through iTunes (at home or at work?) – The user is still involved in the process and considering the history of the laptop – this still creates support calls. This makes sense for the consumer side – not the enterprise side.

Mobile Device Management Choices-

Gartner Webinar: technology_and_management Directions Smartphones and Tablets_kdulaney.pdf - Adobe Acrobat Pro

File Edit View Document Comments Forms Tools Advanced Window Help

Create Combine Collaborate Secure Sign Forms Multimedia Comment

23 / 31 64.4% Find

Mobile Device Management Choices

zenprise
BoxTone
Mobile Service Management

SYBASE

RIM
Proprietary Device Policy + Inventory Management

Mobile Iron
Multi-Device Policy + Inventory Management

Good
Multi-Device Enterprise Containers (various functions)

Multi-Device Unified Applications, Security and Management

Gartner

Security Ratings:

Gartner for Business Leaders Shared - Windows Internet Explorer

http://my.gartner.com/portal/server.pt?open=512&objID=202&mode=2&PageID=5553&ref=webinar-rss&resId=1580214&prm=WB_IPD11R

Convert Select

Favorites myWinCap WinCapWeb Suggested Sites Get More Add-ons

Gartner for Business Leaders Shared

to the consumer market and ultimately to the enterprise. This session will provide a several high level trends for both smartphones and tablets. However the availability of inexpensive yet powerful consumer devices creates a situation where the standards process of the past is no longer an effective strategy for managing enterprise IT integrity. To this end, Gartner will also discuss a replacement for endpoint standards called Managed Diversity.

Download Presentation (PDF, 4.1MB)

Share

View All Upcoming Webinars >

View All Replay Archives >

Media Tablet/Smartphone Management/Security Capabilities

	High-Level Certifications, FIPS, CC, etc.	Application Controls	Vendors' Enterprise Management	Result With Third-Party Management
Apple iOS	✓	Total access control	Apple Back-listing	✓
Android	✓	✓	✓	✓
RIM OS 6, QNX YE11	✓	Core APIs	Custom white-listing	✓
MeeGo	✓	✓	✓	✓
hp WebOS	✓	✓	✓	✓

Gartner

DURATION: 00:47:33 / 01:03:36

PLAYING

Internet | Protected Mode: Off

12:03 PM 4/19/2011

Network Access – the devices need to re-authenticate in less than 100 ms to allow video and telephony. Authentication systems will blend roaming and security in a single model.

Governance and Risk – Must have the following - Acceptable Use Policies, ensure auditors find this utilization as acceptable, insurance compliance; legal compliance should be in place. Xoom and iPad 2 – both have encryption – Honeycomb (post android 2.3) is launched to go encryption **after** the tablet market.

Android IceCream – 3.1 brings together tablet and smartphone together and this will bring in the ability to have security for apps.

Suggestions - If you are not high security agency– you should allow this with jurisdiction because the employees are bringing them anyway.

We could wait and see what Microsoft does is the best decision – **BUT** if you wait that long you will be overwhelmed in the enterprise without governance or control.